

FIG. 1

NETWORK ATTACK PROTECTION SYSTEM

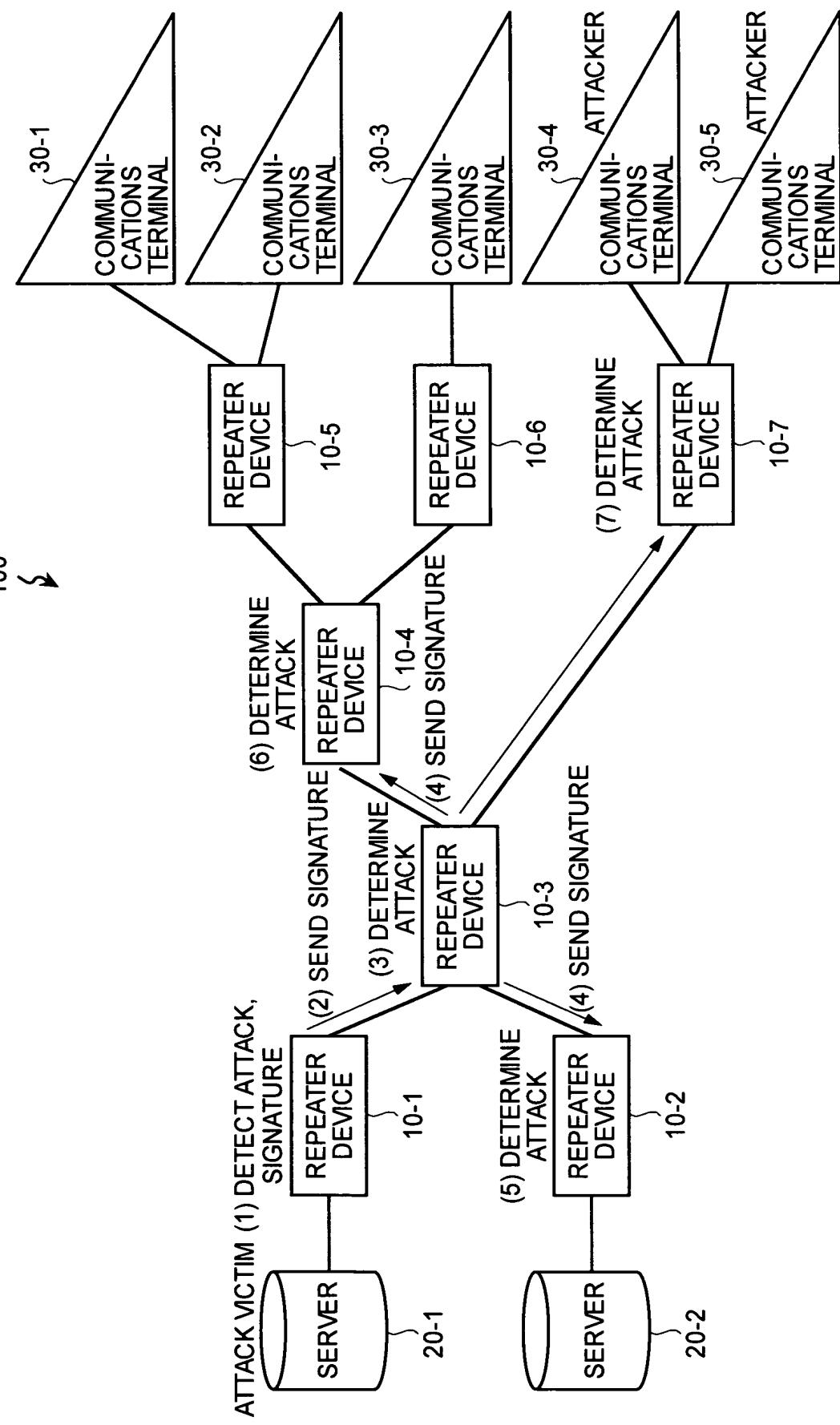


FIG. 2

REPEATER DEVICE
10

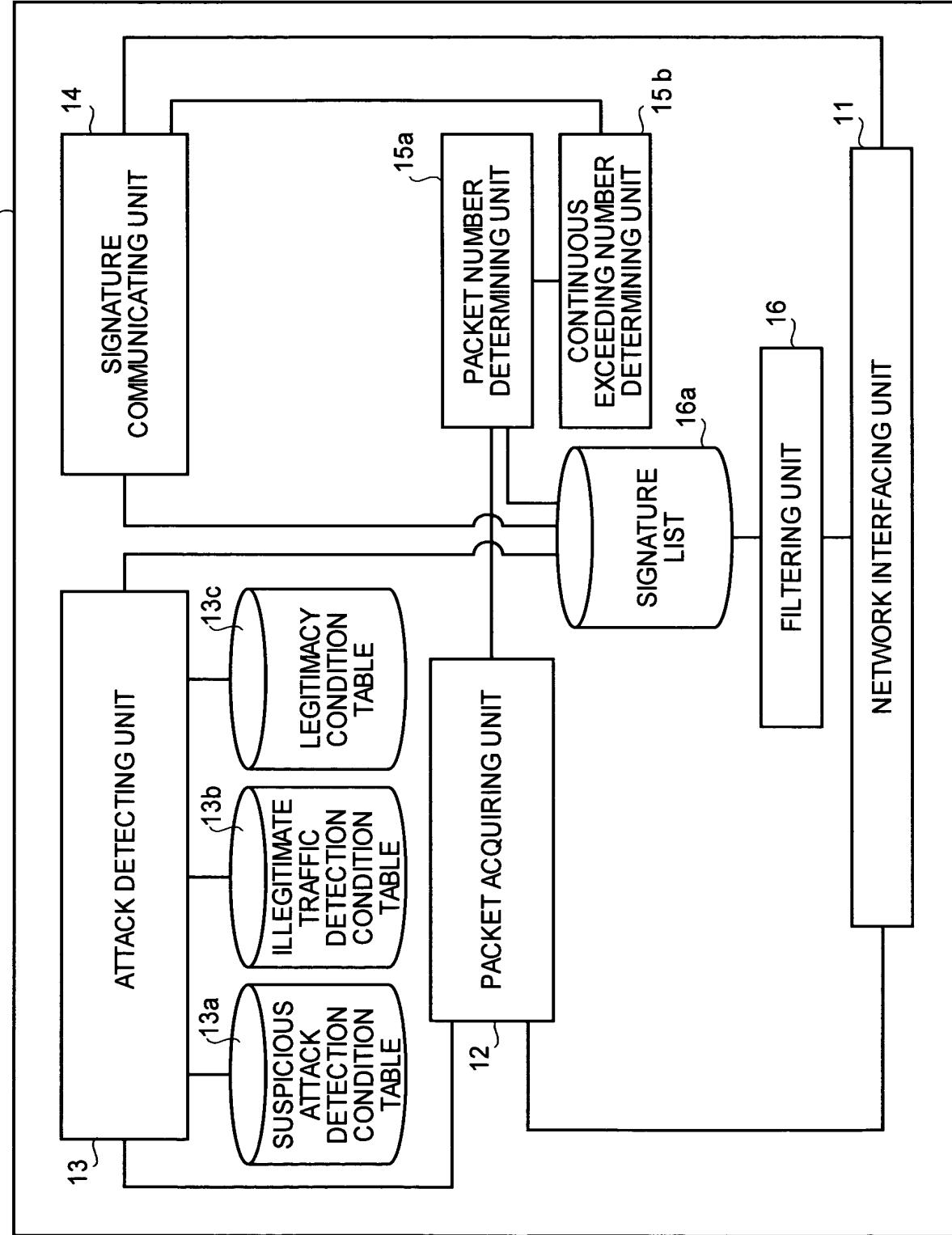


FIG.3

SUSPICIOUS ATTACK DETECTION CONDITION TABLE

13a

NO.	DETECTION ATTRIBUTES	DETECTION THRESHOLD	DETECTION TIME
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500 Kbps	10 SECONDS
2	{Dst=192.168.1.2/32,Protocol=UDP}	300 Kbps	10 SECONDS
3	{Dst=192.168.1.1/24}	1000 Kbps	20 SECONDS
:			

FIG.4

ILLEGITIMATE TRAFFIC DETECTION CONDITION TABLE

13b

NO.	ILLEGITIMATE TRAFFIC CONDITIONS
1	PACKETS AT OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S1 SECONDS OR MORE
2	ICMP/Echo Reply PACKETS AT T2 Kbps OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S2 SECONDS OR MORE
3	FRAGMENT PACKETS AT T3 Kbps OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S3 SECONDS OR MORE
:	

FIG.5

LEGITIMACY CONDITION TABLE

13c

NO.	DETECTION ATTRIBUTES
1	{Src=172.16.10.0/24}
2	{TOS=0x01}
:	

FIG.6

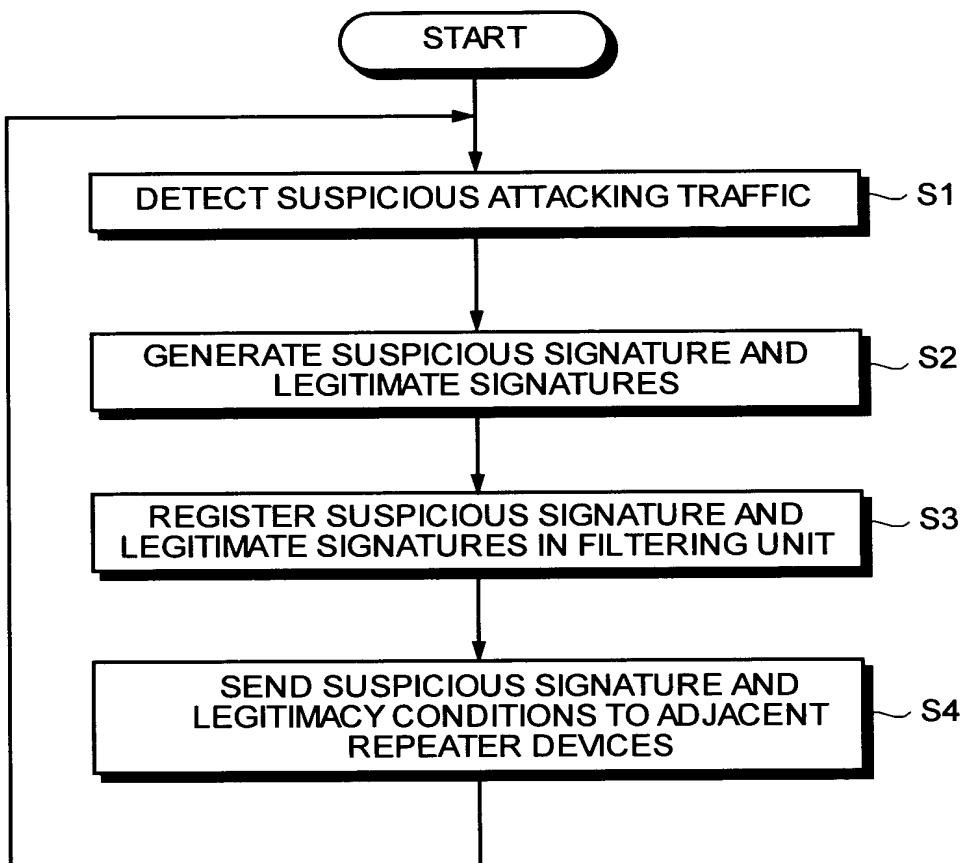


FIG.7

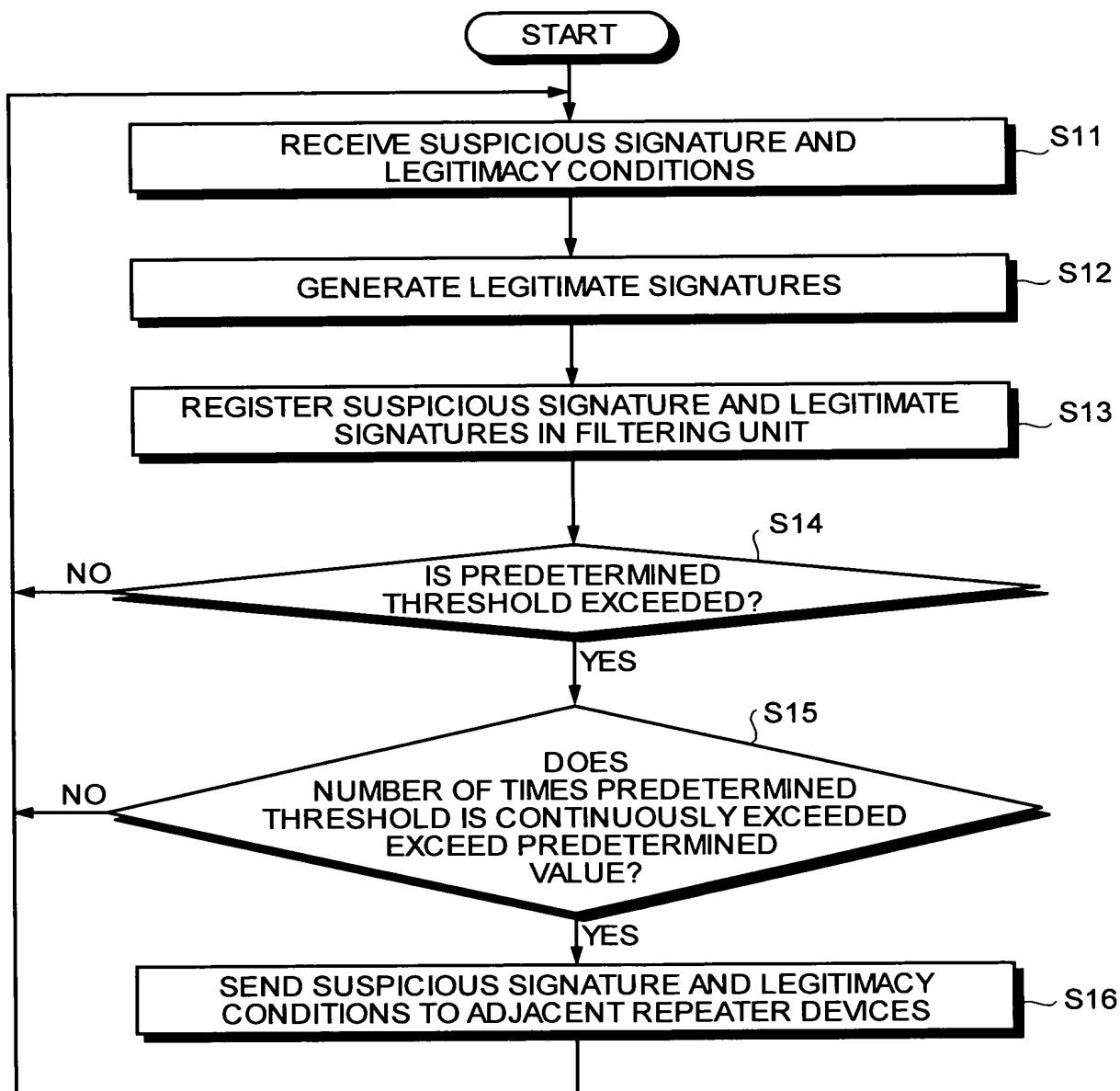


FIG.8

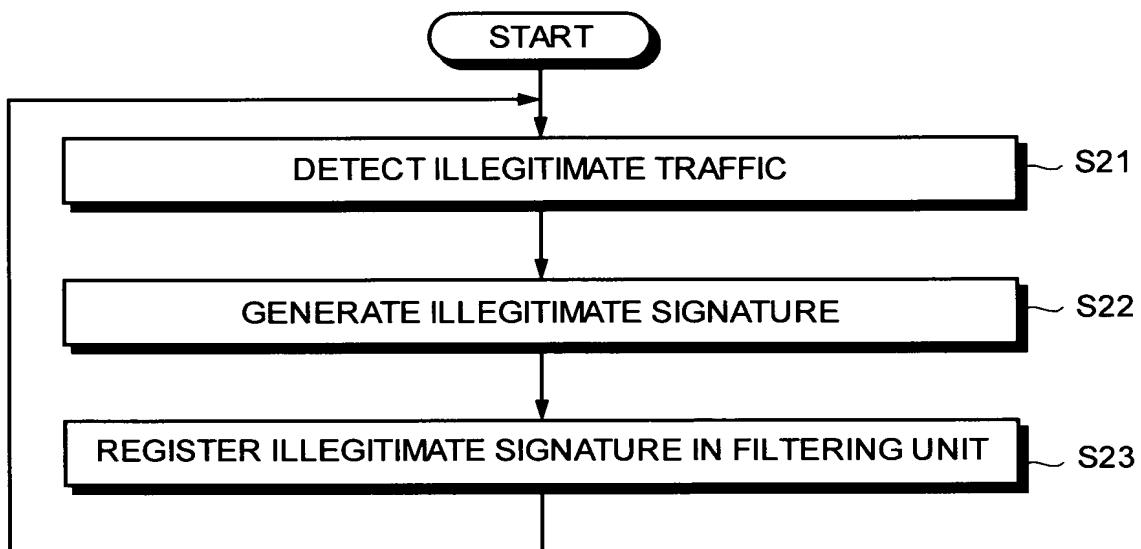


FIG.9

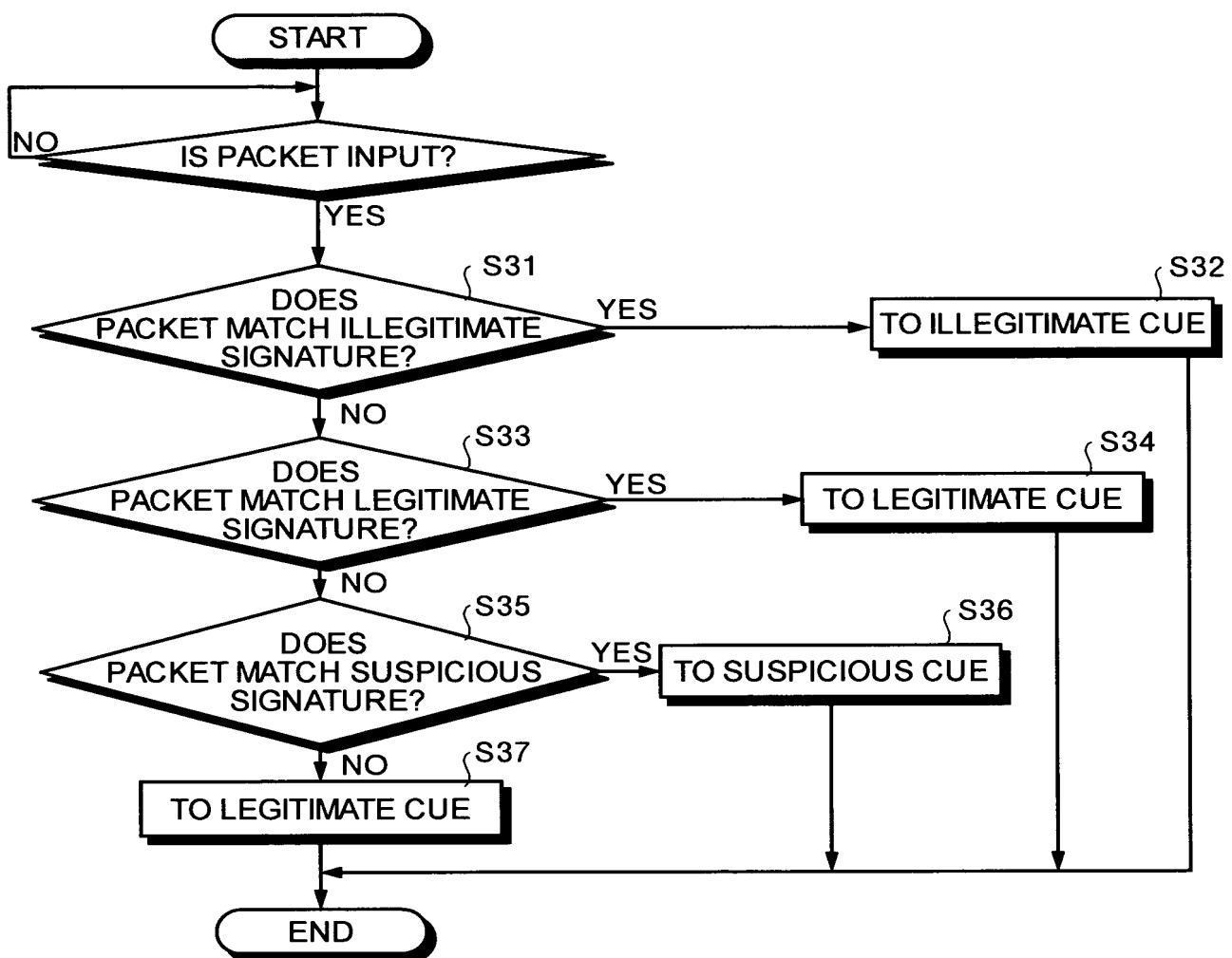


FIG. 10

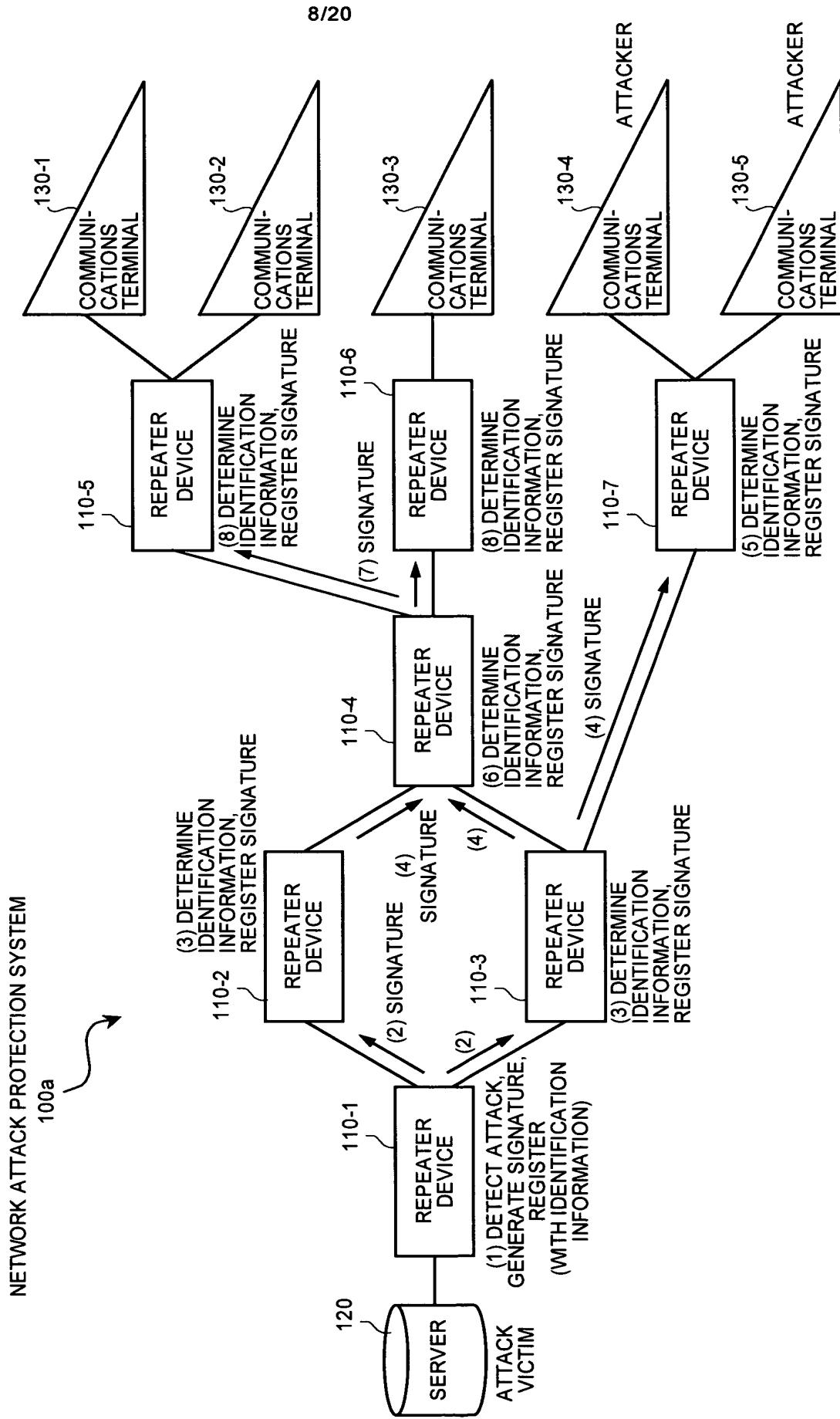


FIG. 11

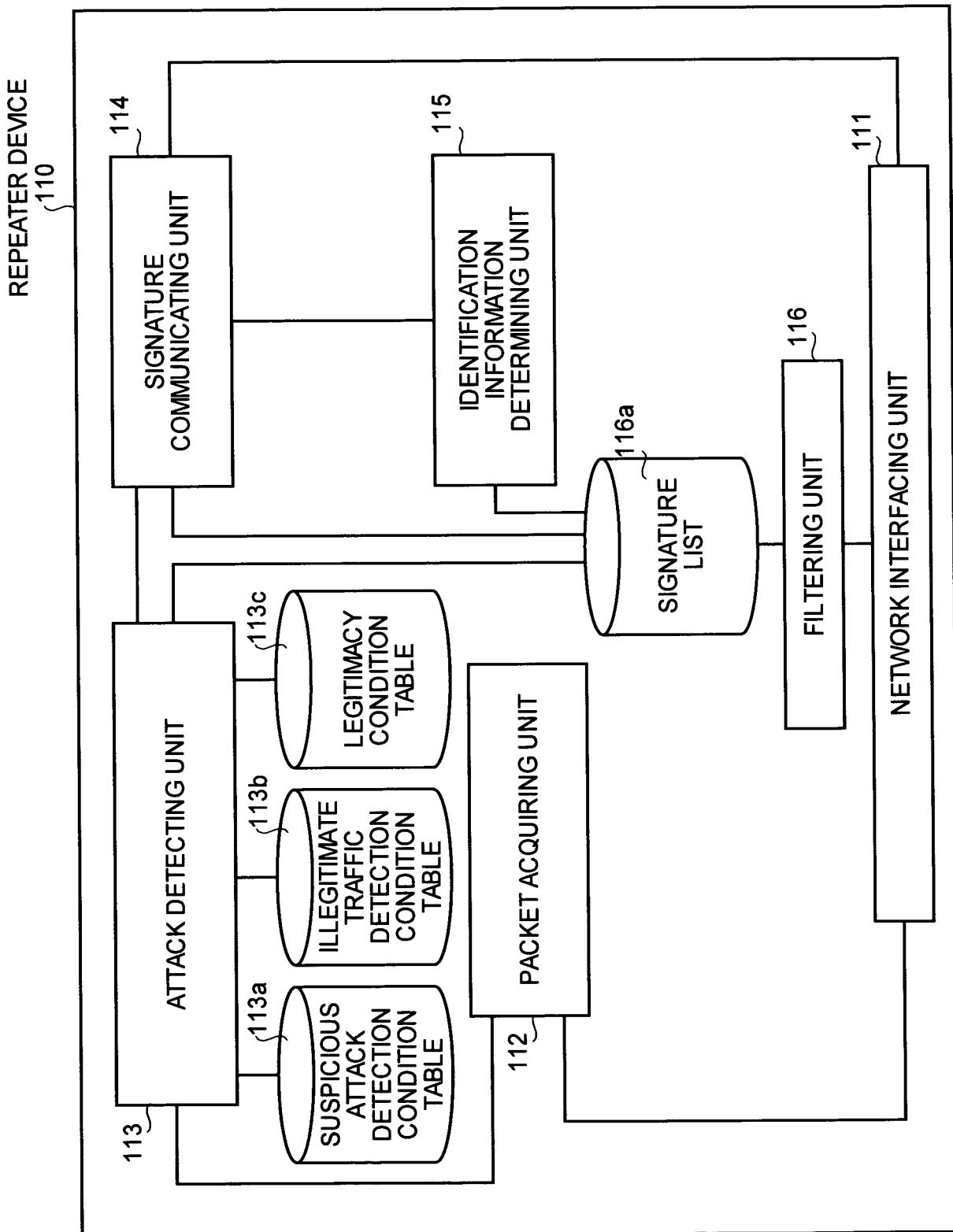


FIG.12

SUSPICIOUS ATTACK DETECTION CONDITION TABLE

113a

NO.	DETECTION ATTRIBUTES	DETECTION THRESHOLD	DETECTION TIME
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500 Kbps	10 SECONDS
2	{Dst=192.168.1.2/32,Protocol=UDP}	300 Kbps	10 SECONDS
3	{Dst=192.168.1.1/24}	1000 Kbps	20 SECONDS
:			

FIG.13

ILLEGITIMATE TRAFFIC DETECTION CONDITION TABLE

113b

NO.	ILLEGITIMATE TRAFFIC CONDITIONS
1	PACKETS AT OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S1 SECONDS OR MORE
2	ICMP/Echo Reply PACKETS AT T2 Kbps OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S2 SECONDS OR MORE
3	FRAGMENT PACKETS AT T3 Kbps OR MORE ARE CONTINUOUSLY TRANSMITTED FOR S3 SECONDS OR MORE
:	

FIG.14

LEGITIMACY CONDITION TABLE

113c

NO.	DETECTION ATTRIBUTES
1	{Src=172.16.10.0/24}
2	{TOS=0x01}
:	

FIG.15

SIGNATURE LIST

116a



SIGNATURE	IDENTIFICATION INFORMATION	DOWNSTREAM NODE	UPSTREAM NODE
SIGNATURE A	(...,...,...,...)	REPEATER DEVICE 10-2	REPEATER DEVICE 10-5,10-6
SIGNATURE B	(...,...,...,...)	REPEATER DEVICE 10-3	REPEATER DEVICE 10-5,10-6
:	:	:	:

FIG.16

IDENTIFICATION INFORMATION {LOCAL ALERT ID,ENGINE-TYPE,ENGINE-ID,NODE-ID}

- LOCAL ALERT ID: IDENTIFIER OF UNIQUE ALERT IN ANALYSIS ENGINE
- ENGINE-TYPE: IDENTIFIER OF ANALYSIS ENGINE TYPE
- ENGINE-ID: IDENTIFIER OF SAME ANALYSIS ENGINE BELONGING TO SAME MITIGATION
- NODE-ID: NODE IDENTIFIER OF MITIGATION TO WHICH ANALYSIS ENGINE BELONGS

FIG.17

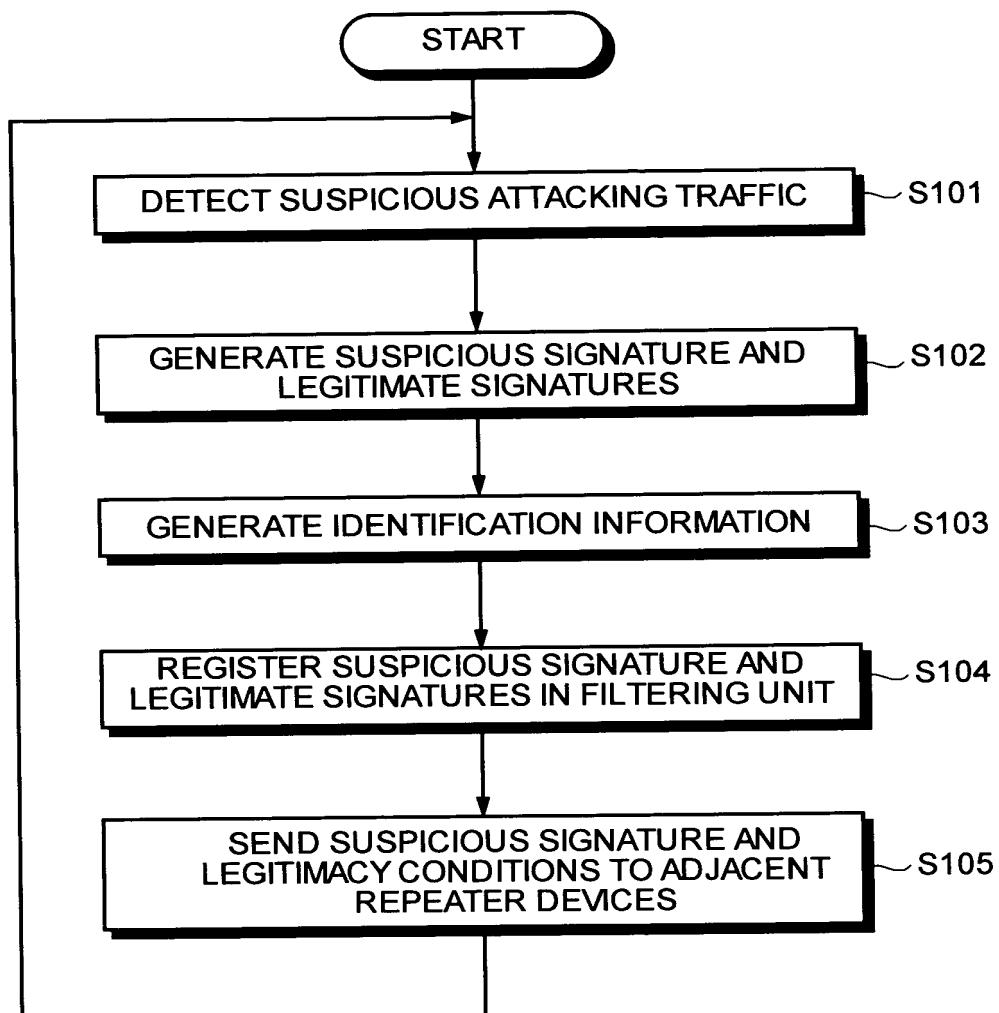


FIG.18

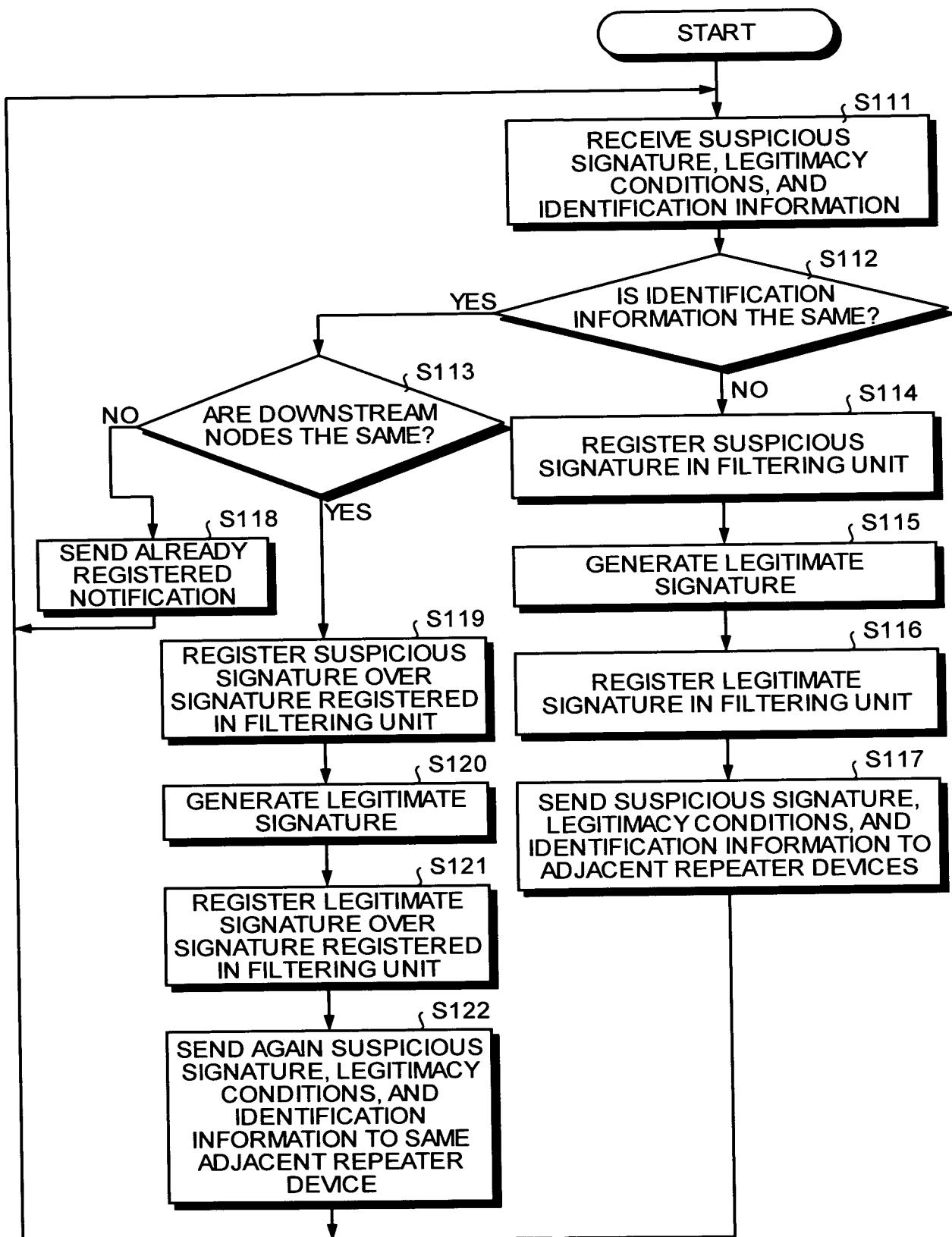


FIG. 19

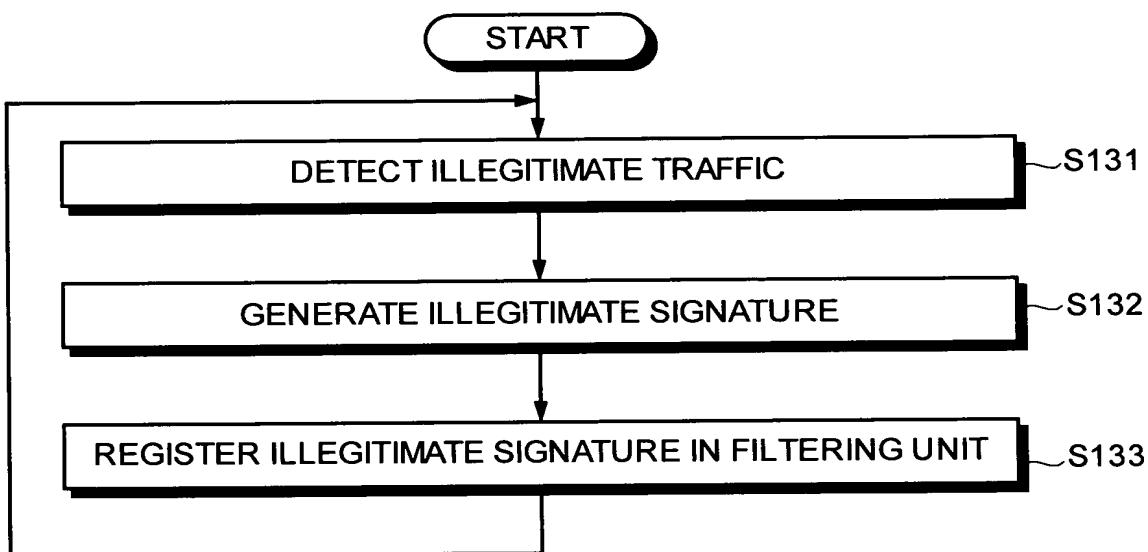


FIG.20

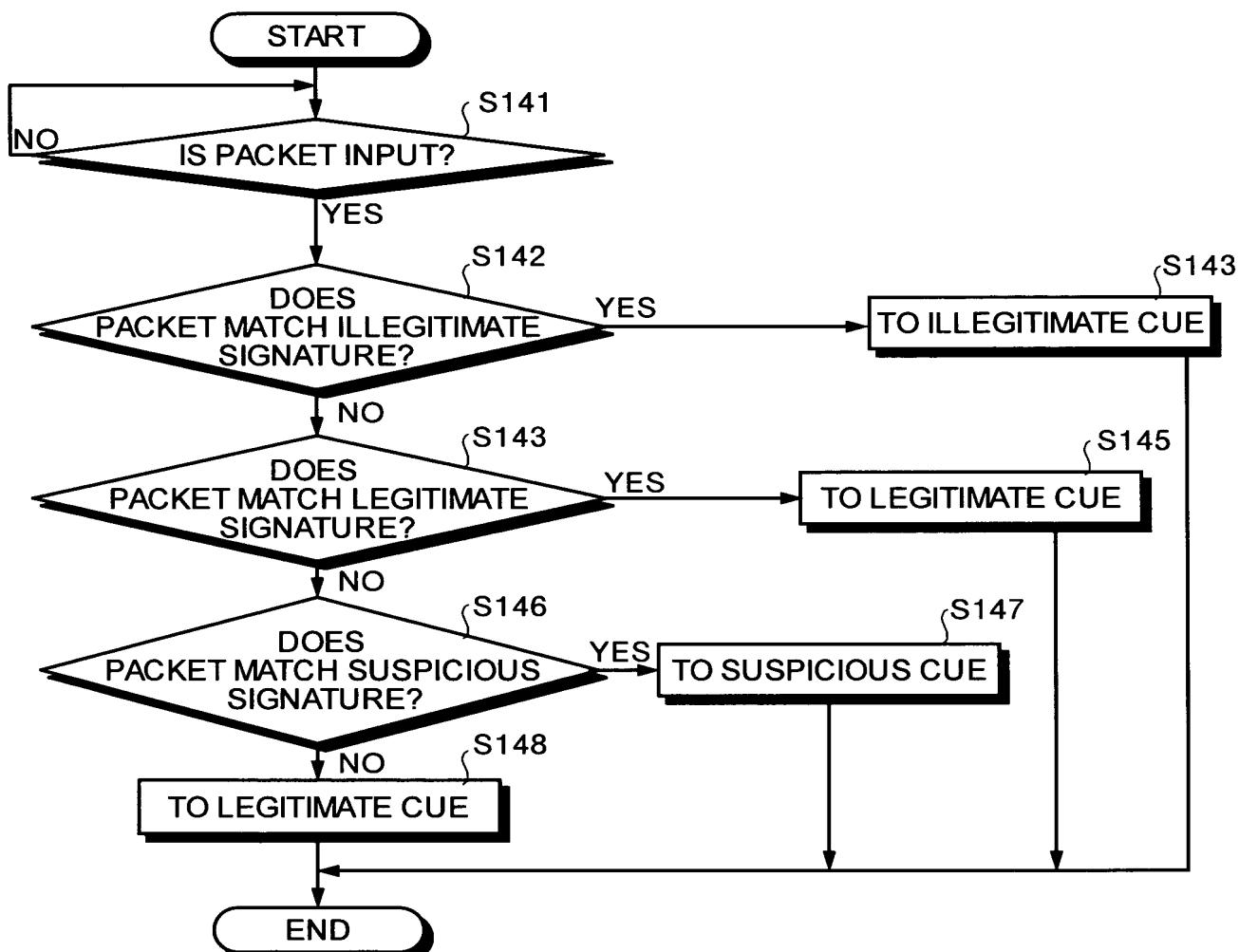


FIG.21

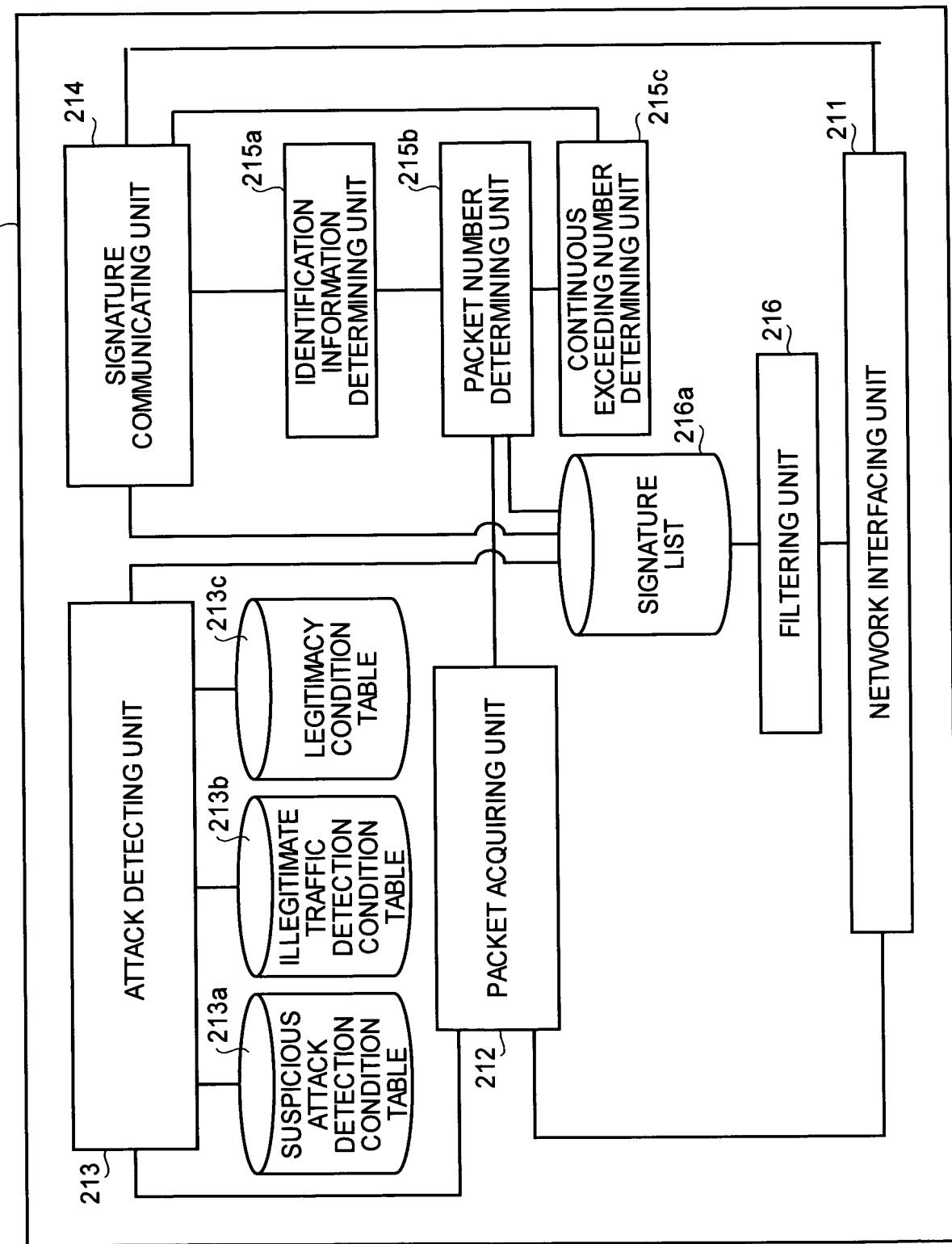


FIG.22

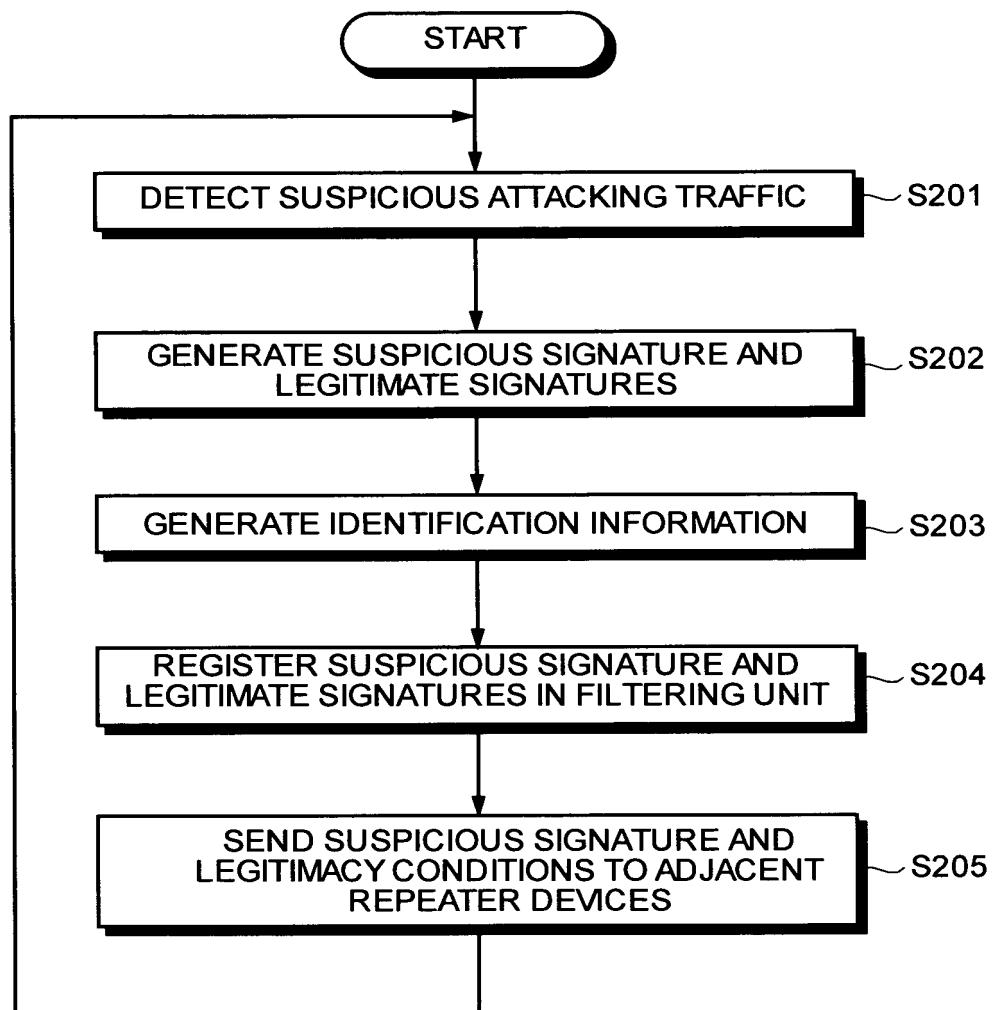


FIG.23

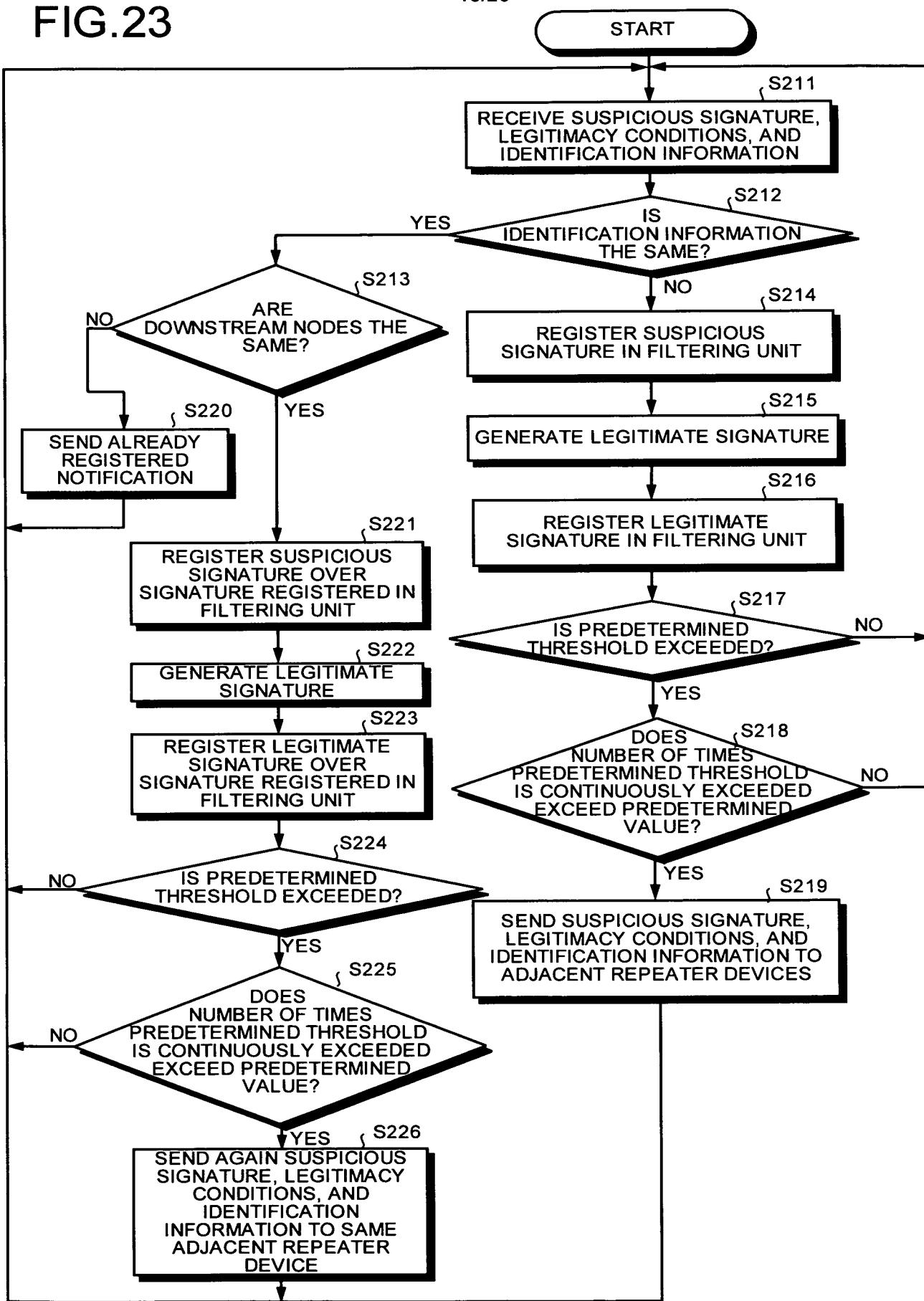


FIG.24

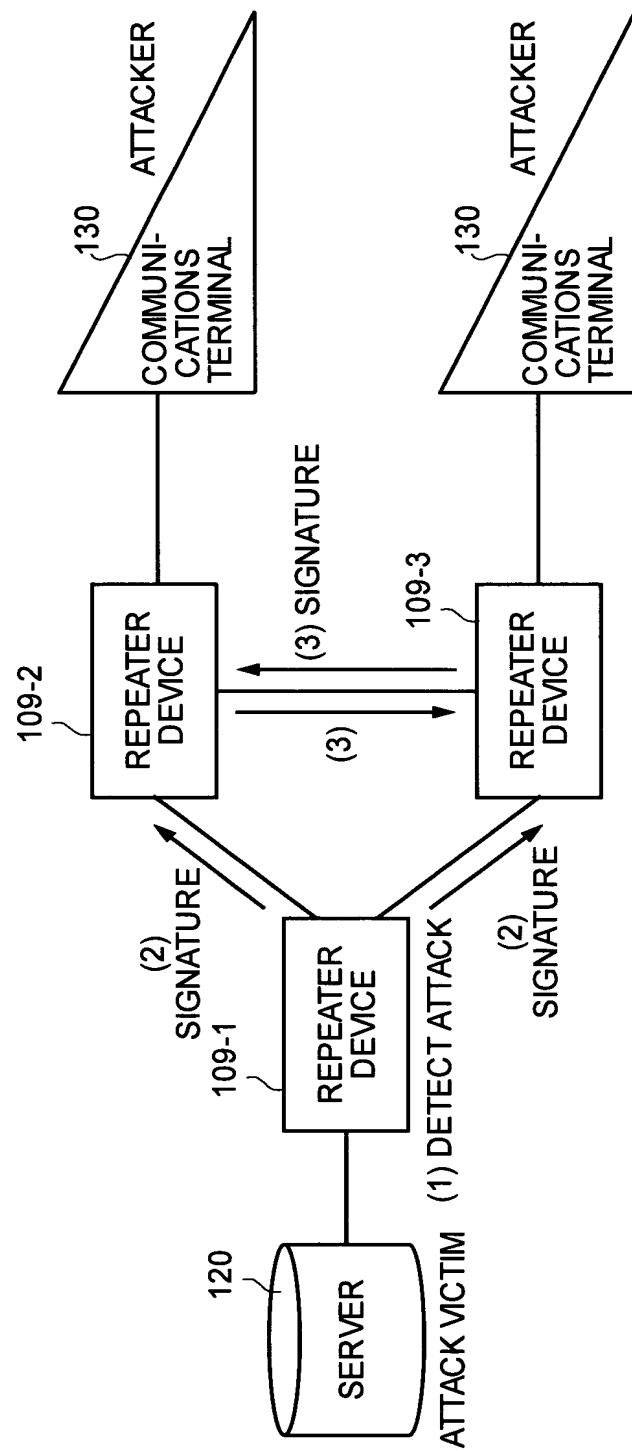


FIG. 25

